

 What makes you special?

IBM ISS

*Managed
Security
Services*



*Professional
Services*

*Security
Hardware and
Software*



IBM Internet Security Systems



Copyright 2004 by Randy Glasbergen.
www.glasbergen.com



**“If I can put everyone to sleep within the first five minutes,
the rest of my presentation should go pretty well.”**

Meldung vom 28.04.2009

Demo-Exploits für neue Schwachstellen im Adobe Reader

Im Internet zirkulieren Demo-Exploits für zwei neue Sicherheitslücken im Adobe Reader. Laut der SecurityFocus-Fehlerdatenbank sind Versionen 9.1 und 8.1.4 des PDF-Anzeigers betroffen. Einen Patch für die Schwachstellen gibt es bislang noch nicht. Mit der Veröffentlichung der Demo-Exploits steigt die Wahrscheinlichkeit enorm, dass PDF-Dokumente mit gefährlichem Schadcode auftauchen und die Lücken auf breiter Front ausgenutzt werden.

Only IBM Security is Backed by the IBM X-Force® Research Team

Research

Technology

Solutions

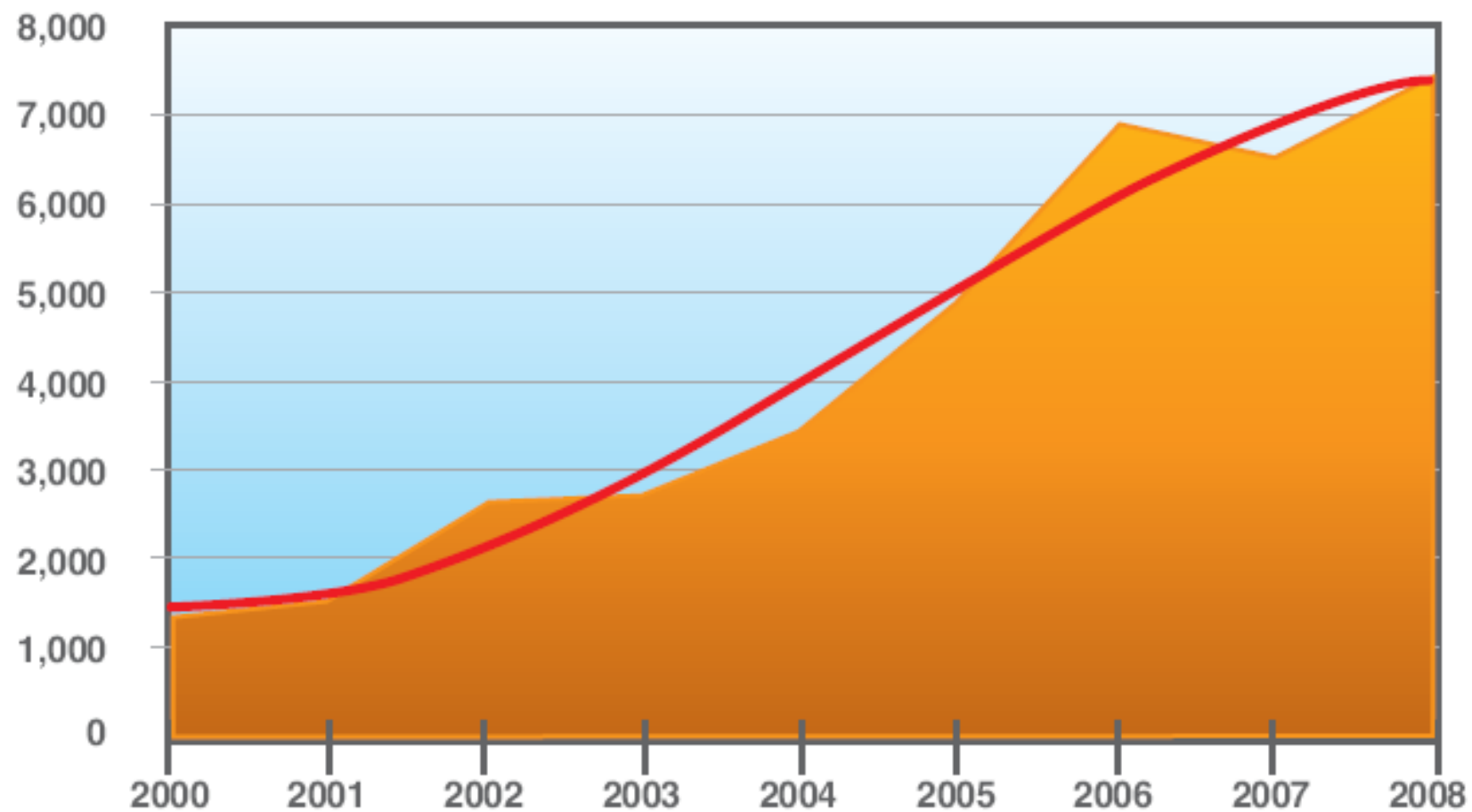


- X-Force Protection Engines**
 - Extensions to existing engines
 - New protection engine creation
- X-Force XPU's**
 - Security Content Update Development
 - Security Content Update QA
- X-Force Intelligence**
 - X-Force Database
 - Feed Monitoring and Collection
 - Intelligence Sharing



The X-Force team delivers reduced operational complexity – helping to build integrated technologies that feature “baked-in” simplification

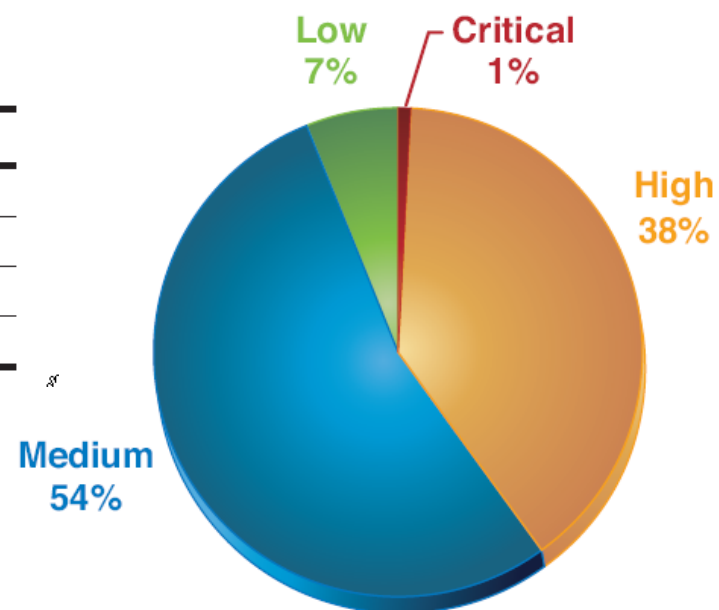
Schwachstellen im Jahresvergleich :



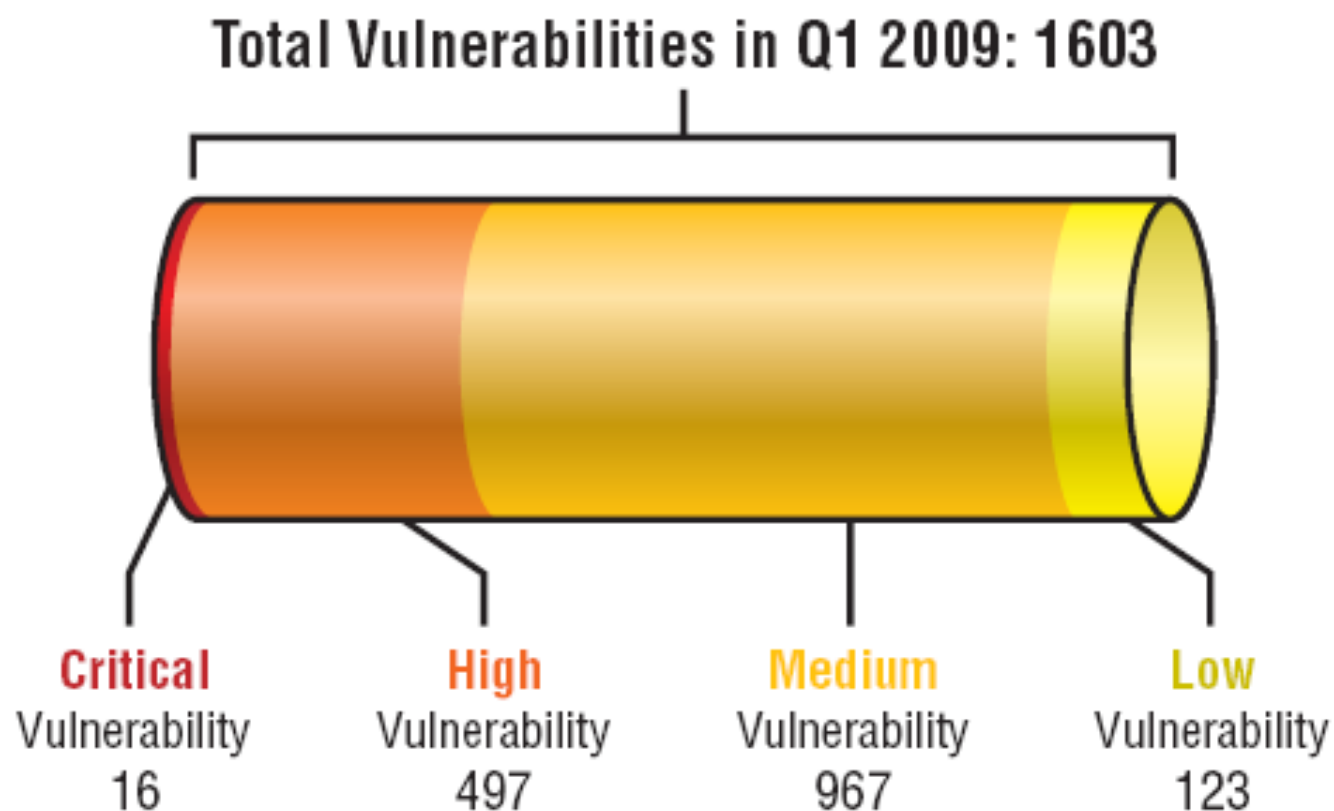
R

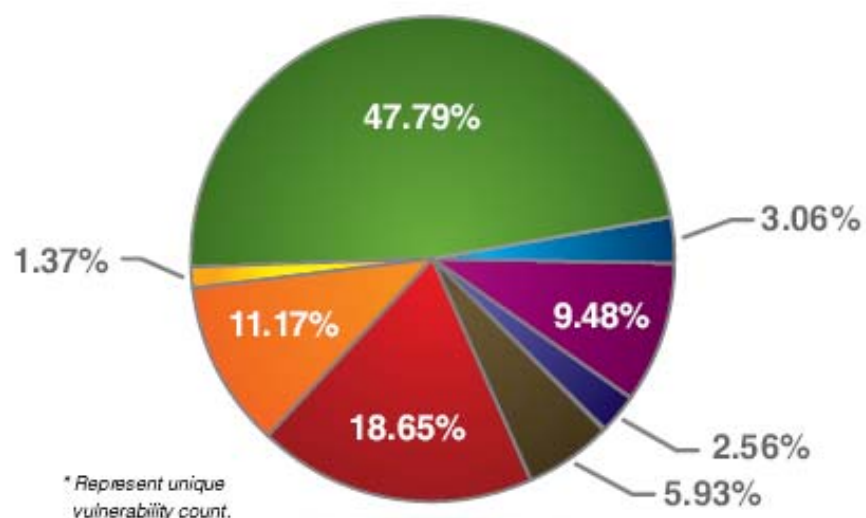
Ranking of the Vulnerabilities

Year	Busiest Week for Vulnerability Disclosures
2000 – 2005	Week before Christmas
2006	Week before Thanksgiving
2007	Summer
2008	Week before Christmas



Total Vulnerabilities in Q1 2009: 1603





Bypass Security – 5.93%

Circumvent security restrictions such as a firewall or proxy, and IDS system or a virus scanner.

Data Manipulation – 18.65%

Manipulate data used or stored by the host associated with the service or application.

Denial of Service – 11.17%

Crash or disrupt a service or system to take down a network.

File Manipulation – 1.37%

Create, delete, read, modify, or overwrite files.

Gain Access – 47.79%

Obtain local and remote access. This also includes vulnerabilities by which an attacker can execute code or commands, because this usually allows the attacker to gain access to the system.

Gain Privileges – 3.06%

Privileges can be gained on the local system only.

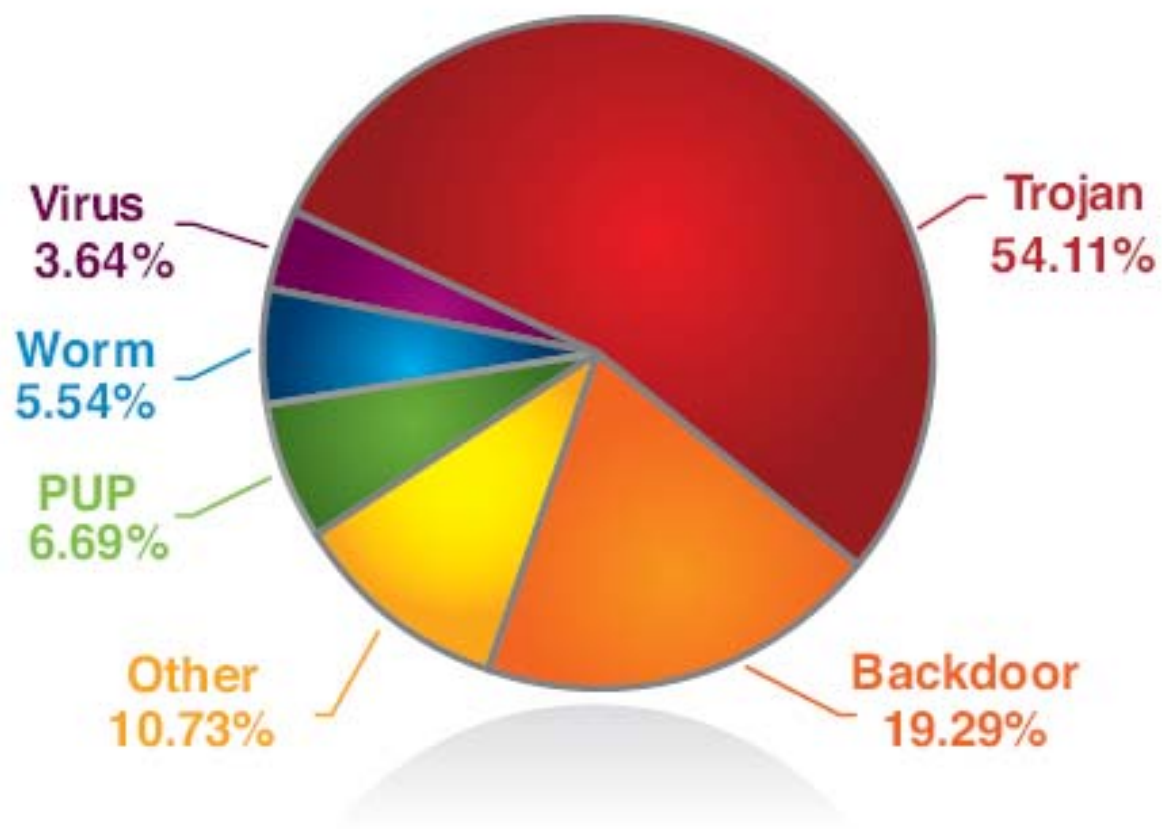
Obtain Information – 9.48%

Obtain information such as file and path names, source code, passwords, or server configuration details.

Other – 2.56%

Anything not covered by the other categories.

Malcode corner



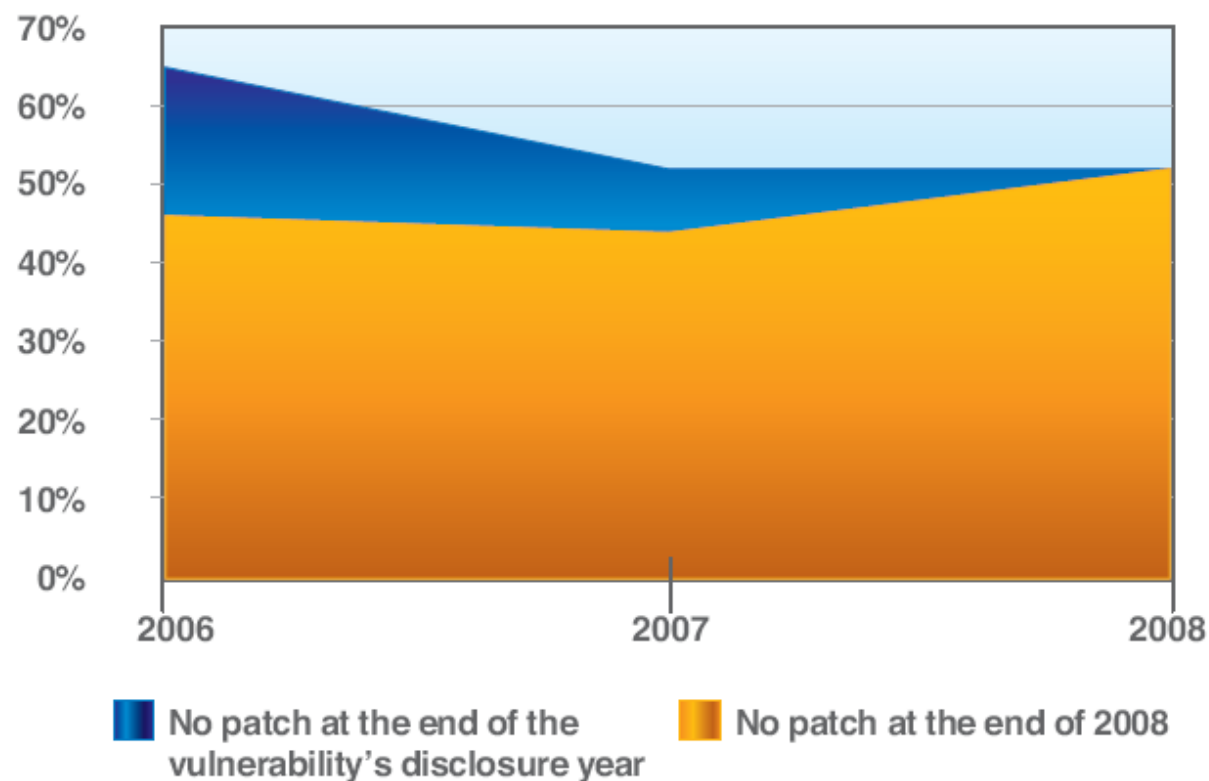
Vendors with the Most Vulnerability Disclosures

Ranking	Vendor	Disclosures
1.	Microsoft	3.16%
2.	Apple	3.04%
3.	Sun	2.19%
4.	Joomla!	2.07%
5.	IBM	2.00%
6.	Oracle	1.65%
7.	Mozilla	1.43%
8.	Drupal	1.42%
9.	Cisco	1.23%
10.	TYPO3	1.23%

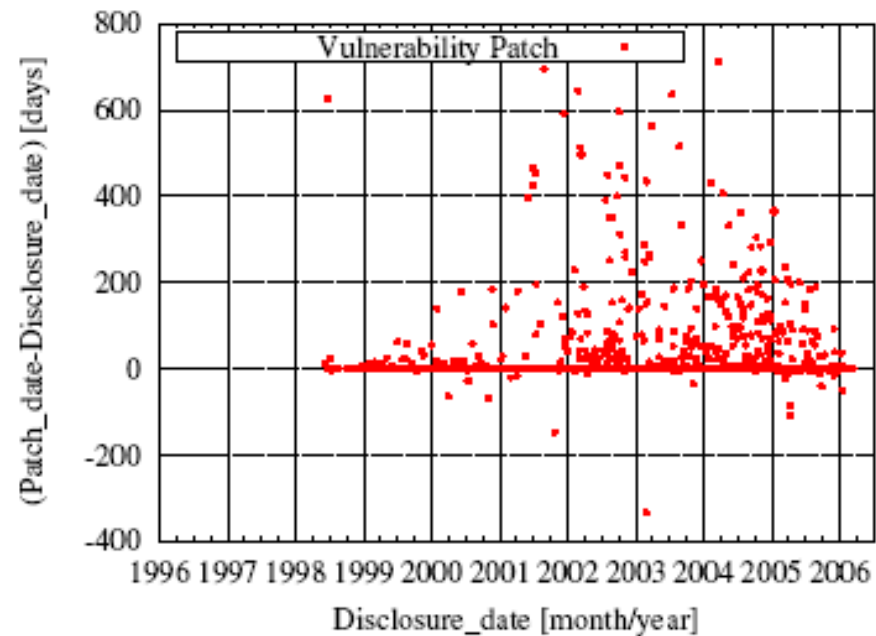
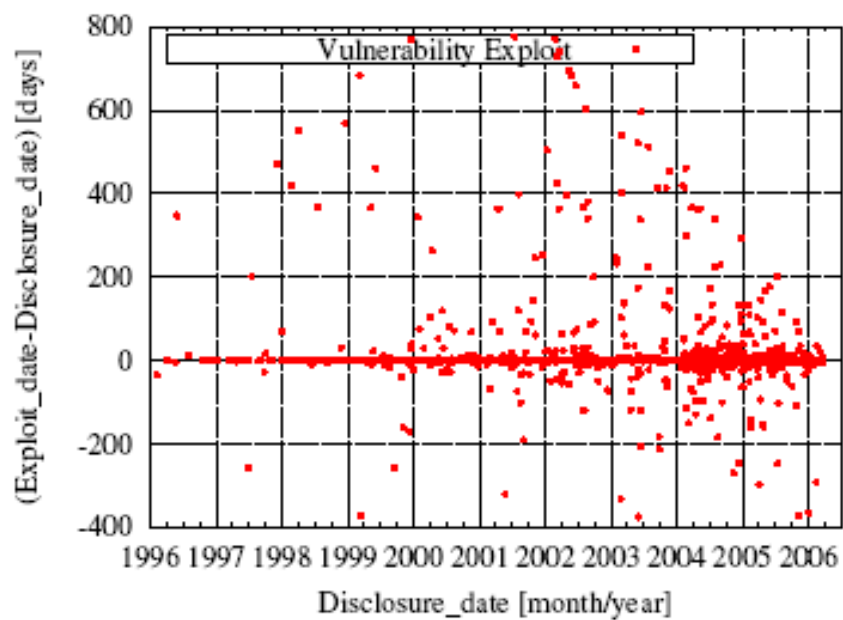
Table 3: Vendors with the Most Vulnerability Disclosures

Availability of Vulnerability Fixes and Patches

At the end of 2008, 53 percent of all vulnerabilities disclosed during the year had no vendor-supplied patches available to remedy the vulnerability. Vendors do not always go back to patch previous year's vulnerabilities. 46 percent of vulnerabilities from 2006 and 44 percent from 2007 were still left with no available patch at the end of 2008.



Vulnerabilitys

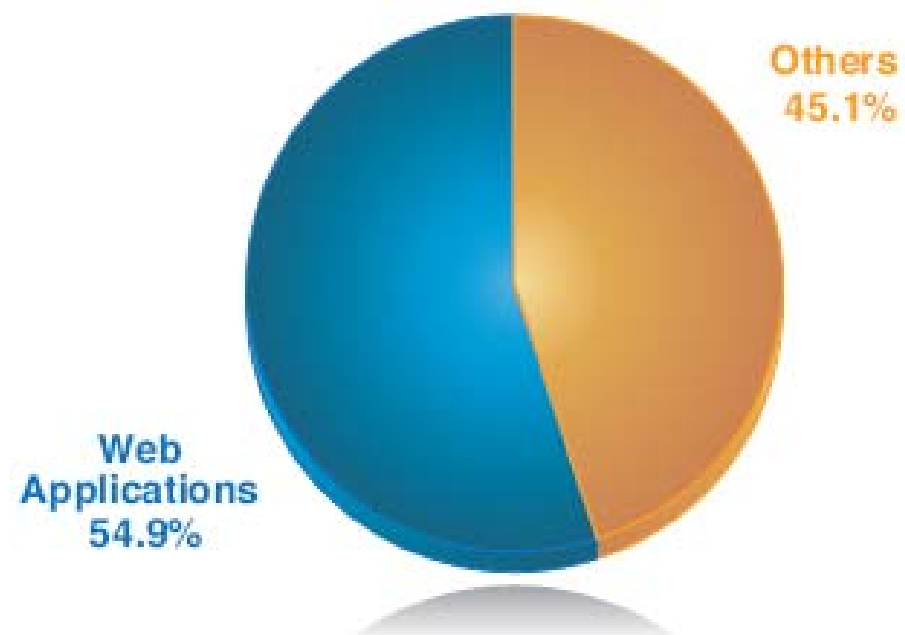


Exploits

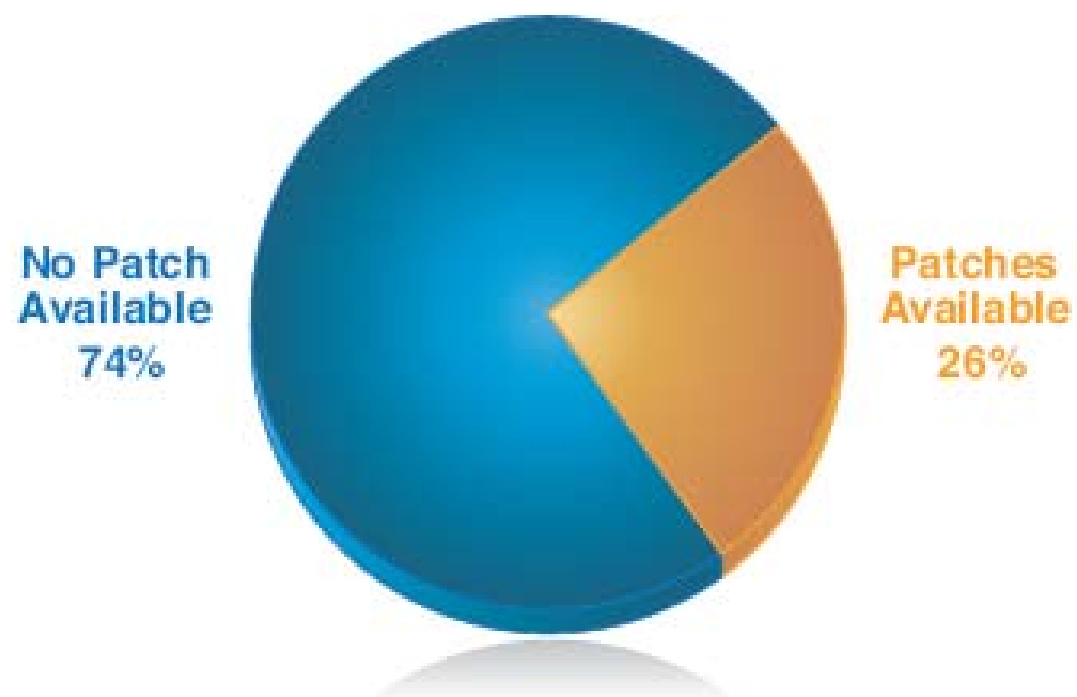
e Tools

	<p style="text-align: center;">Bronze Edition</p> <ul style="list-style-type: none"> ■ This product is the improved version of Turkojan 3.0 and it has some limitations(Webcam - audio streaming and msn sniffer doesn't work for this version) ■ 1 month replacement warranty if it gets dedected by any antivirus ■ 7/24 online support via e-mail ■ Supports only Windows 95/98/ME/NT/2000/XP ■ Realtime Screen viewing(controlling is disabled) <p>Price : 99\$ (United State Dollar)</p>
	<p style="text-align: center;">Silver Edition</p> <ul style="list-style-type: none"> ■ 4 months (maximum 3 times) replacement warranty if it gets dedected by any antivirus ■ 7/24 online support via e-mail and instant messengers ■ Supports 95/98/ME/NT/2000/XP/Vista ■ Webcam streaming is available with this version ■ Realtime Screen viewing(controlling is disabled) ■ Notifies chngements on clipboard and save them <p>Price : 179\$ (United State Dollar)</p>
	<p style="text-align: center;">Gold Edition</p> <ul style="list-style-type: none"> ■ 6 months (unlimited) or 9 months(maximum 3 times) replacement warranty if it gets dedected by any antivirus (you can choose 6 months or 9 months) ■ 7/24 online support via e-mail and instant messengers ■ Supports Windows 95/98/ME/NT/2000/2003/XP/Vista ■ Remote Shell (Managing with Ms-Dos Commands) ■ Webcam - audio streaming and msn sniffer ■ Controlling remote computer via keyboard and mouse ■ Notifies chngements on clipboard and save them ■ Technical support after installing software ■ Viewing pictures without any download(Thumbnail Viewer) <p>Price : 249\$ (United State Dollar)</p>

Web Application Vulnerabilities



No Patch for You



Embedded Systems



Defining Pre-Emption - What's the Difference?

Protecting against exploits is reactive:

- Too late for many
- Variants undo previous updates
- Typical of antivirus and most IDS/IPS vendors

Protecting against vulnerabilities and behaviors is proactive:

- Stops threat at source
- Requires advanced R&D



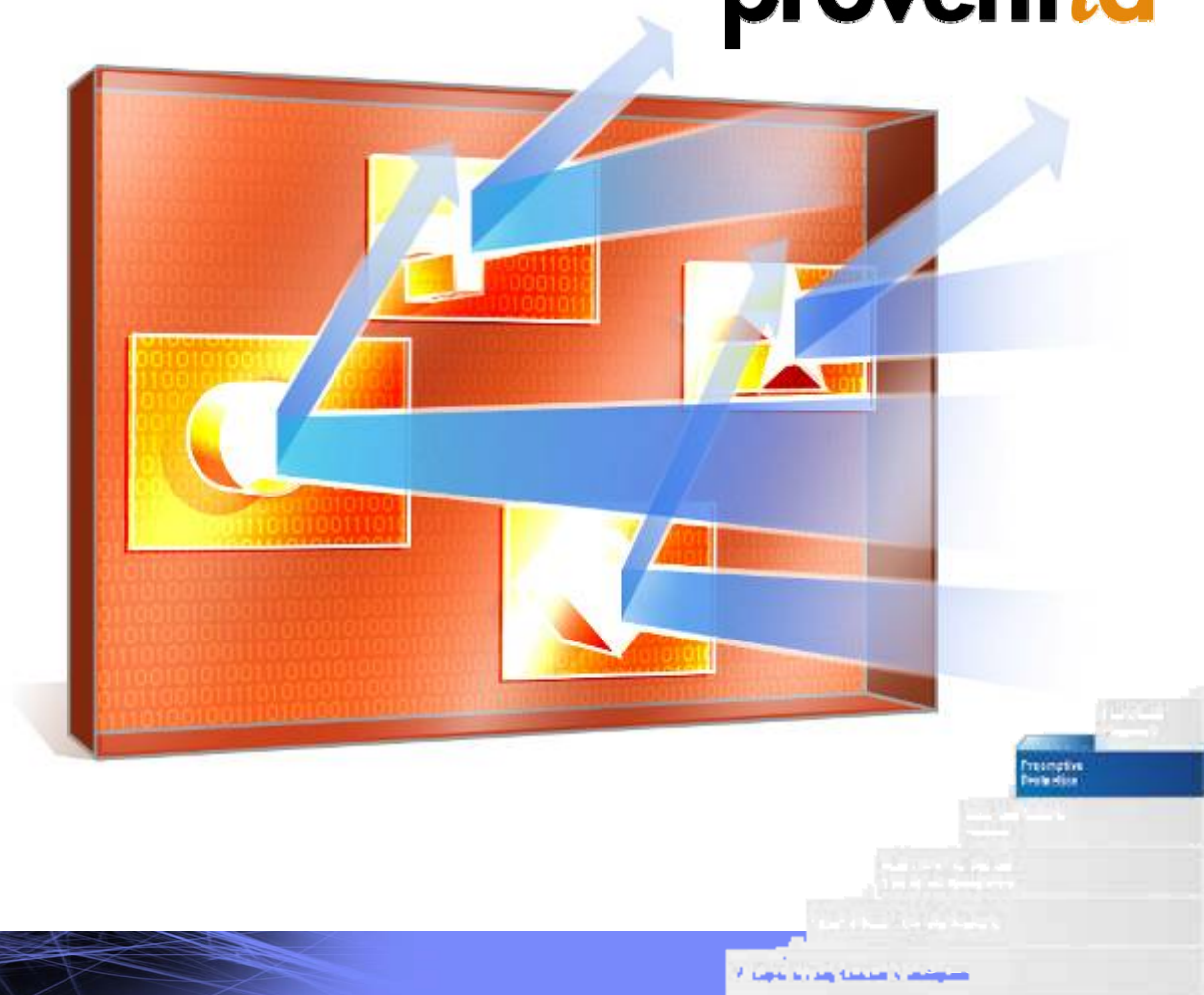
Präventive Sicherheit durch - Virtual Patch



proventia™

*Proventia bietet ein
Schutzschild
“Virtual Patch”
für bekannte
Schwachstellen*

- “Virtuelle Patches” schützen vor sofortiger Ausnutzung bekannter Schwachstellen
- Reduziert das Risiko durch Beeinflussung der IT-Prozesse
- Patchen kann geplant durchgeführt werden



Microsoft Bulletin MS08-067

IBM ISS 2 years *Ahead of the Threat*



The IBM ISS Virtual Patch protects customers until they can download and install security updates from their software vendor.



Stefan Klett
Channel Account Manager
Internet Security Systems
Vulkanstrasse 106
8010 Zürich
+41 (58) 333 7901 (Office)
+41 (79) 617 7069 (Mobile)
stefan.klett@ch.ibm.com

Questions?

